REPUBLIC OF TÜRKİYE

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Electrical and Computer Engineering

CYBERSECURITY RISK ASSESSMENT FOR UNMANNED AIRCRAFT SYSTEMS

Eymen ELRIFAI

Master's Thesis

Supervisor

Asst. Prof. Dr. Muhammad ILYAS

Istanbul, 2022

CYBERSECURITY RISK ASSESSMENT FOR UNMANNED AIRCRAFT SYSTEMS

Eymen Elrıfaı

Electrical and Computer Engineering

Master's Thesis

ALTINBAŞ UNIVERSITY

2022

The thesis titled CYBERSECURITY RISK ASSESSMENT FOR UNMANNED AIRCRAFT SYSTEMS prepared by EYMEN ELRIFAI and submitted on 20/12/2022 and has been **accepted unanimously** for the degree of Master of Science in Electrical and Computer Engineering.

____

Asst. Prof. Dr. Muhammad ILYAS

Supervisor

Thesis Defense Committee Members:

Asst. Prof. Dr. Muhammad ILYAS	Department of Computer Engineering, Altınbaş University	___________________
Asst. Prof. Dr. Abdullahi abdu IBRAHIM	Department of Computer Engineering, Altınbaş University	___________________
Asst. Prof. Dr. Jawad RASHEED	Department of Software Engineering, Nişantaşı University	___________________

I hereby declare that this thesis meets all format and submission requirements of a Master's thesis.

Submission date of the thesis to Institute of Graduate Studies: ___/___/___

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Eymen Elrıfaı

ABSTRACT

CYBERSECURITY RISK ASSESSMENT FOR UNMANNED AIRCRAFT SYSTEMS

Elrıfaı, Eymen,

M.Sc. Electrical and Computer Engineering, Altınbaş University,

Supervisor: Asst. Prof. Muhammad ILYAS

Date: December/2022

Pages: 33

Today, cybersecurity and safety are two of the most pressing operations in UAS development. There has been a lot of work put in by legislators and aviation authorities to ensure that UAS operations inside the existing airspace system are safe. Specific Operation Risk Assessment (SORA) is a methodology developed by the Joint Authorities for Rulemaking on Unmanned Aircraft Systems (JARUS). This methodology may be used as a risk for assessing the assessments associated with Specific Category UAS operations. However, only a subset of safety-related issues may be addressed by the methodology. This document details the steps we took to adapt the SORA methodology for use in the field of cybersecurity. To demonstrate this strategy, we broaden the methodology to include the secrecy challenge On the areas of official government buildings and military and security areas, which is a part of cybersecurity.

Keywords: Cybersecurity, UAS, SORA, Specific Operation Risk assessment, Secrecy

TABLE OF CONTENTS

Pages

LIST OF TABLES

LIST OF FIGURES

Pages

ABBREVIATIONS

AOV	:	Angle Of View
ARC	:	Air Risk Class
BVLOS	:	Beyond Visual operation of Sight
CONOPS	:	Concept of Operations
EASA	:	European Aviation Safety Agency
EC	:	European commission
EU	:	European Union
GRC	:	Ground Risk Class
ICAS	:	Industrial Control and Automation System
JARUS	:	Joint Authorities for Rulemaking on Unmanned Systems
OSO	:	Operational Safety objectives
SAIL	:	Specific Assurance and Integrity Levels
SORA	:	Specific Operation Risk Assessment
SRC	:	Secrecy Risk Class
UA	:	Unmanned Aircraft
UAV	:	Unmanned aerial vehicle
UAS	:	Unmanned Aircraft System
VLOS	:	Visual operation of Sight operations

1. INTRODUCTION

1.1 CONTEXT

First deployed as targets in the late 1900s [2], UAVs have been around for quite some time. UAS markets have emerged since then. Civilian uses of UAS were overlooked in favor of military ones until recently. This includes situations like reconnaissance and battle. The unmanned aircraft system (UAS) industry for civilian uses has been expanding since the 2000s. Initially, civilians used unmanned aircraft mostly as toys for private recreation. Then, technological advancements (such as increasing computing power, improving sensor battery capacity, and miniaturizing components) make UASs more compact and appealing for professional and commercial uses across a wide range of economic sectors, including photography/media, transportation, energy, agriculture, etc. [3]. In the recent decade, the market for civil UAS has expanded dramatically. A total of over $3 billion will be spent in this space between 2012 and 2019 as the market expands from $2 billion in 2016 [4] to $14.1 billion in 2018 [5].

Many groups and market research firms have projected sales for civil UAS in the future. When you include in the seven million recreational drones, approximately 400,000 commercial drones will be flying over Europe by 2050, according to the SESAR Joint Undertaking [6]. Estimates put the value of the civil drone industry at $70 billion by 2027 [7]; this is from Market Research Future.

According to research by Drone Industry Insights [4, the civil drone industry is expected to be worth $43.1 billion by 2024. The market is expected to be worth $15 billion by 2022, according to research firm Interact Analysis [8]. Although these figures are simply estimates, they are optimistic overall. These projections, in other words, show how optimistic investors are about the future of the civilian drone sector. However, there are still barriers that prevent this market from being fully exploited. Current rules, which restrict the use of UASs for reasons like security, safety, and secrecy, are one of the most pressing problems [9].

To deal with the development of UAS operations and to provide a legal framework for UAS, European lawmakers first examined UASs with more than 150 kg takeoff weight in Regulation (EC) No 216/2008, and then all kinds of UASs in the new Regulation (EU) 2018/1139. These guidelines provide the groundwork for the whole civil aviation sector. The 2018/1139 rule establishes the risk-based technique to construct a regulatory framework for UAS operations. In light of this, it follows that rules and procedures for UAS operations should be adjusted to account for the specific dangers involved in each mission. Delegated Regulation (EU) 2019/945 and Implementing Regulation (EU) 2019/947 were published by the European Commission in 2019 to maintain uniformity with preexisting legislation. They include specific guidelines for things like certification, EU operators, operators from other nations, communication systems and UAS design [10]. These guidelines are outlined in accordance with the operating categorization suggested by the European Aviation Safety Agency (EASA). Open, Specific, and Certified are the three types of operations depending on risk [11]. To acquire operational authorizations for "Specific" and "Certified" activities, risk assessments must be conducted in accordance with Implementing Regulation 2019/947. The "Specific" risk assessment, which includes the vast majority of commercial UAS activities, is of particular importance to this project. In addition, the scope of the risk assessment should go beyond that of aircraft safety. In addition to covering the dependency between safety and cybersecurity/secrecy [10, 12], it should also take into account the safety of other domains depending on the operating setting (such as communications, infrastructures, transportation, and so on).

1.2 RELATED WORKS AND CONTRIBUTION

Common steps in any given risk assessment include "risk analysis", “risk identification" and "risk evaluation." Many different methods have been devised for doing these jobs. There has been discussion of risk assessment methods in the realm of safety since the 1940s. There are now over a hundred distinct approaches [13]. Fault Tree Analysis (FTA), HAZOP, Fault Mode, Markov analysis, and Bow-tie analysis, Effect Analysis (FMEA), and Petri-nets analysis are some common and commonly used ones. Meanwhile, risk assessment in cybersecurity was first studied somewhere.

The broad use and increasing interconnectedness of digital systems began in the late 1980s. There are several connections between safety and cyber security. The primary difference between the two is that "safety" deals with risks associated with accidents while "security" deals with risks associated with malevolent activities or assaults. [14], [15], [16], [17]. As a result, many cybersecurity risk assessment methods take cues from their counterparts in the safety industry.

Failure Mode and Effects Analysis (FMEA) [21] is the progenitor of both Attack Tree Analysis (FTA) [18] and Intrusion Modes and Effects Analysis (IMEA) [20]. Markov analysis [20] and Petri-net analysis [21] are made safe despite being fundamentally dangerous approaches. And there's a trend toward harmonizing safety risk assessment with cyber risk assessment. An FTA-based integrated technique was proposed by Kornecki et al. [22] for an air traffic management system; an FMEV-based integrated technique was proposed by Schmittner [23] and illustrated in the context of an Industrial Control and Automation System (ICAS); and Abdo [24] proposed a technique to deal with uncertainties in a risk assessment that incorporated both safety and security.

In addition to specific methods, safety and security focused industrial standards and methodologies have been established and implemented to serve as comprehensive frameworks for a variety of sectors. For example, there is the IEC 61508 standard [25] for the security of E/E/PE systems, the ARP4761 standards [26] for the security of avionic systems, the ISO 27000 standard series [27] for the security of information systems, the IEC 62443 standard [28] for the cybersecurity of ICAS, the EVITAD project [29] for networked automobile systems, the DO-326 standard [30] for the cybersecurity of avionic systems, etc.. Industry attention is now being paid to integrated approaches to safety and security. By way of illustration, Specifically, the ARP4761 standard's safety-based methodology was expanded in the DO-326 standard so that it could be used to the field of Cybersecurity. The IEC 63187 standard, which is an expansion of IEC 61508 standard, was being created to better adapt to the growth of contemporary technology and to account for the cybersecurity element [31]. Specific Operation Risk Assessment (SORA) is a technique recognized in 2018 by the European Union Aviation Safety Agency as meeting the requirements for risk assessment as set out in Implementing Regulation 2019/947 for unmanned aircraft system (UAS) operations. Users are given instructions on how to do a risk assessment using this methodology. In order to determine what kinds of precautions are necessary for a certain UAS safety, users need just look at the tables in this handbook. However, the documentation for this program does a poor job of explaining its central notion. While this approach

does address concerns about physical safety, it does not address cybersecurity in the context of operating certain UAS [32]. As a result, we want to broaden the scope of the SORA approach to include considerations of cyber security in the sites of official buildings and military locations. Here's how the rest of the report is laid out. Section 2 explains the basic idea behind the SORA approach. In Section 3, we provide a strategy for expanding the technique. In Section 4, we provide an expansion of the SORA methodology to account for the harm of secrecy. We provide a case example in Section 5. In the last section, we briefly review our results and provide some suggestions for where future studies should go.

2. SORA METHODOLOGY EXPLANATION

The National Aviation Authorities - Joint Authorities for Rulemaking on Unmanned Systems (JARUS) suggested the Specific Operations Risk Assessment (SORA) [33, 34, 35] , a holistic and operation centric methodology. Safety objectives (in system performance, training, development, and organization) may be better understood for every specific UAS operation with the use of this framework. Several groups of interested parties could benefit from this technique. This technique might be used by aviation authorities and operators (who fly the UAS) to ensure compliance with EU legislation and facilitate communication during administrative procedures. The SORA methodology might be used by manufacturers (who design and build UAS) to ascertain the safety aspects that their designs must attain for certain activities. We outline the overall idea of the methodology, which consists of a risk model and an assessment procedure, below.

2.1 RISK MODEL

Bow-tie models (Figure 1) are used in the SORA technique to depict the potential outcomes of the many risks that are taken into risk. For even a fundamental familiarity with the process, knowledge of the model is required. The key components of this framework are the following: (1) a hazard; (2) harms; (3) threats; and (4) barriers.

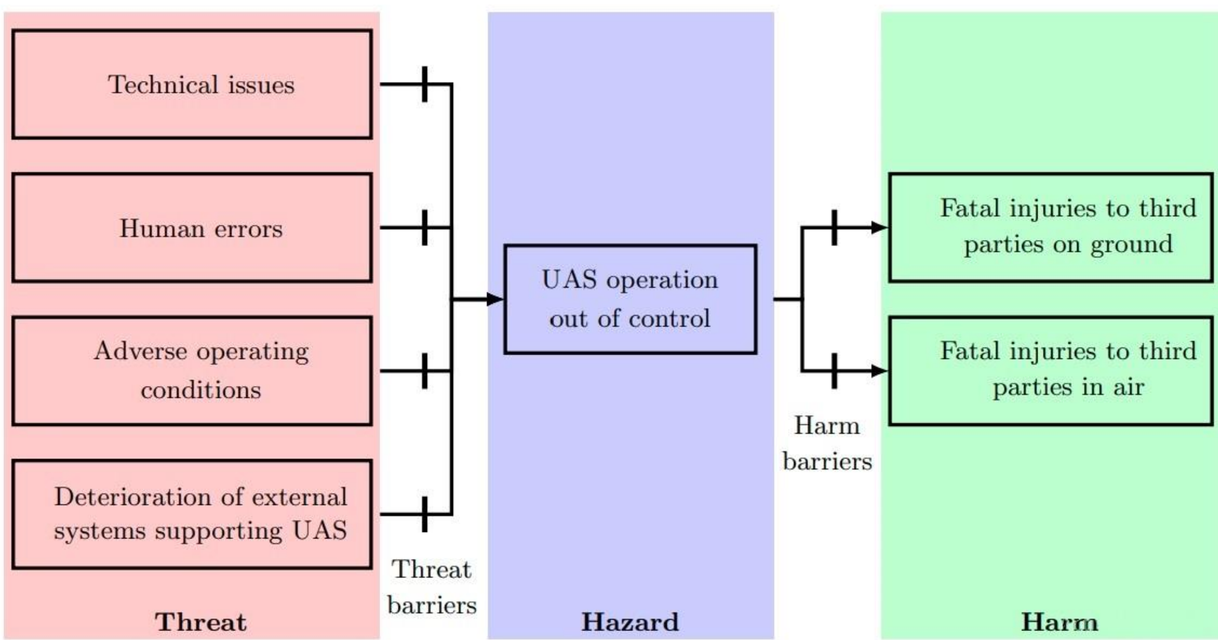

Figure 2.1: Risk analysis using the SORA methodology, shown as a bow-tie diagram

The Bow-Tie Graph revolves around the Hazard. In this context, "unintentional operation" means that a task is completed without the operator's knowledge or consent (In a Visual Line Of Sight operation, for instance, this may mean that the plane is flying out of the pilot's line of sight.) Figure 2.1: The SORA methodology's bow-tie diagrammatic portrayal of the risk model.

To the left of the hazard is where you'll find the Threats. You may look at them as potential sources of the technical issues Human errors Adverse operating conditions Deterioration of external systems supporting UAS operation out of control Fatal injuries to third parties on ground Fatal injuries to third parties in air Threat Hazard Harm hazard. Due to the fact that the SORA methodology is only concerned with safety, only a subset of accidental threat categories is shown in the bow-tie graph (Figure 2.1).

3) Right next to the Hazard is a list of possible outcomes, or Harms. Currently, the SORA methodology only takes into account two types of injury to human life: “fatal injuries to third parties in air" and "fatal injuries to third parties on land,"(see Figure 1). As can be shown in Figure 2.2, the likelihood of each Harms may be broken down into three parts. Likelihood of fatal injuries on the air and in the ground, Figure 2.2 [32].

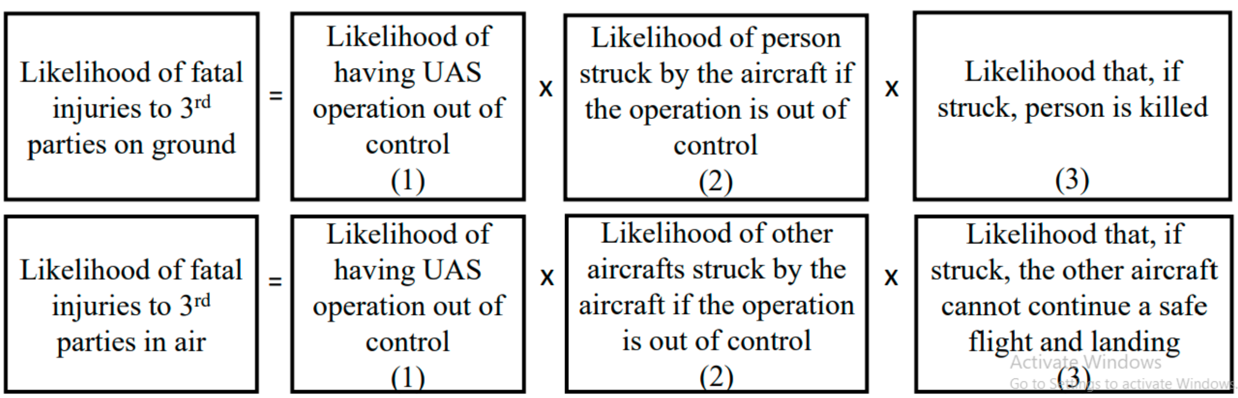

Figure 2.2: Likelihood of Fatal Injuries on the Ground and in the Air [32]

4) The two main categories of barriers are the harm barrier and the threat barrier. Once a Hazard has occurred, Harm barriers stop more harm from happening. In other words, we may reduce the value of items (2) and (3) in Figure 2 by using the Harm barriers. Barriers to possible hazard reduce the likelihood of an incident involving a hazard. In other words, thanks to the Threat barriers, the likelihood of an uncontrolled UAS operation (element (1) in Figure 2) is reduced. At the conclusion of the risk assessment, specific Threat barriers in the form of Operational Safety objectives will be

established for each threat category (OSO). Three distinct levels of robustness are described for each OSO (Low, Medium, High). To illustrate, OSO includes "the UAS is designed following to design standards recognized by authorities" [36]. The applicant must meet varying criteria depending on the desired level of this OSO's robustness. The application must merely state that minimum requirements have been met in order to be considered at the low robustness level. To demonstrate conformity with the stated criteria, the applicant must present supporting evidence (such as analysis or simulation results) at the medium robustness level. To achieve a high level of robustness, the supporting evidence must be verified by independent experts. Following this, we detail the risk model upon which the SORA methodology's assessment is based.

2.2 ASSESSMENT PROCESS

In Figure 3 we can see how the SORA methodology suggests a qualitative way for the assessment. Here's how one possible justification for this method goes.

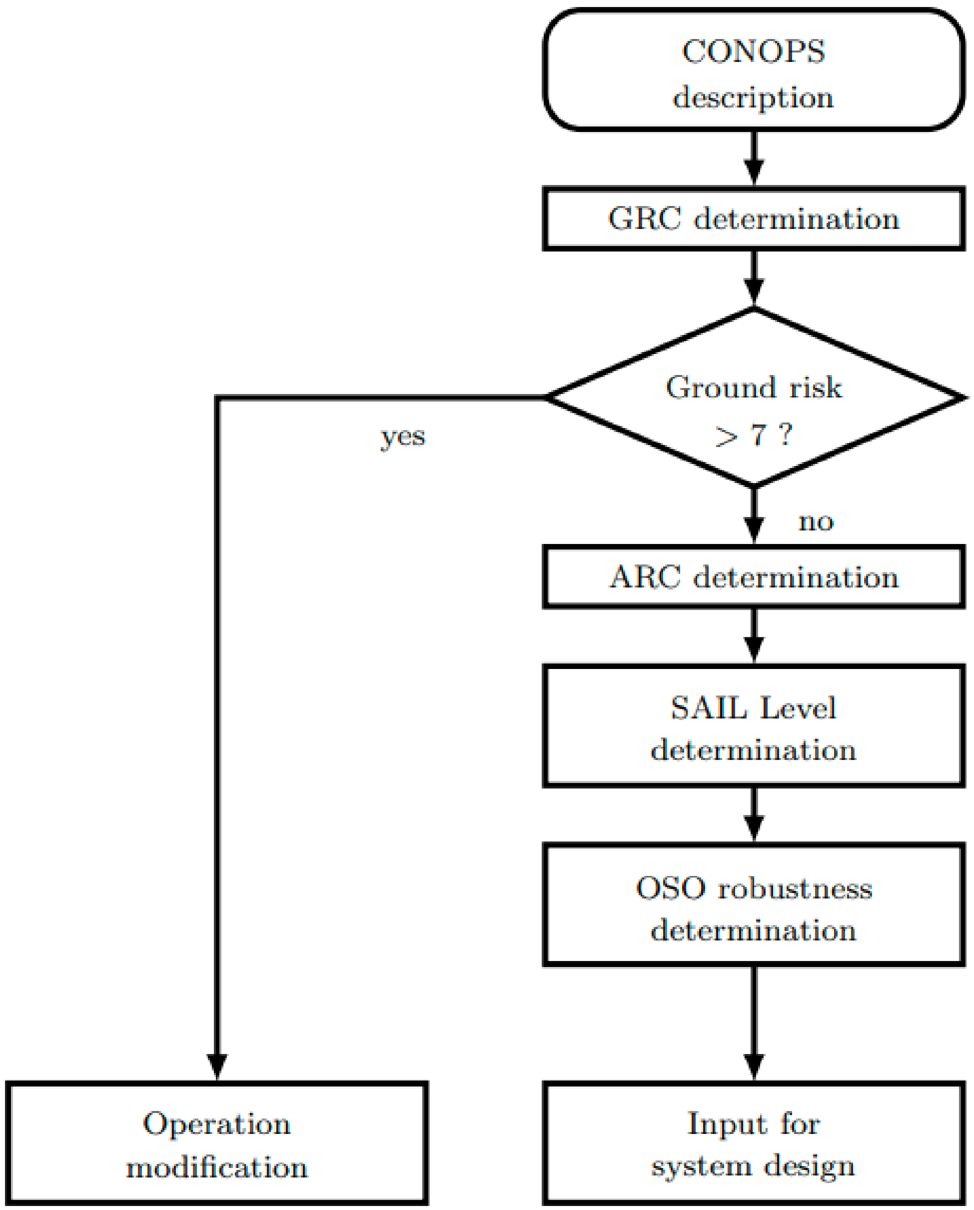

Figure 2.3: Simplified risk assessment process

1) Objective: In the event of a UAS operation, it is essential that we keep the likelihood of each harm below a certain threshold.

2) Initially, we draft a Concept of Operations (CONOPS) description to gather data about the planned action.

3) As a second step, we quantify the GRC importance (Ground Risk Class). This number shows the possibility that a person on the ground may be hurt as a result of an uncontrolled UAS operation. The components (2) and (3) of the first equation in Figure 2 are combined to get this number. When calculating the GRC, we take into account both the inherent characteristics of the operation and any existing Threat obstacles. We are able to ascertain the true worth of GRC based on its inherent properties, such as aircraft characteristics and the operating environment (see Table 1). We then use the Threat barriers to revise the GRC's ultimate value. A parachute, by way of illustration, is a threat barrier that serves to mitigate harm to onlookers on the ground. Having a certified parachute on board would allow us to lower the GRC number. The official SORA paper [37] provided the specifics on Threat barriers.

Table 2.1 : shows the SORA methodology's intrinsic GRC metrics

Intrinsic Ground Risk Class				
Max vehicle dimension	1 m	3 m	8 m	>8 m
Operation scenario				
VLOS/BVLOS over controlled ground area	1	2	3	4
VLOS in sparsely populated environment	2	3	4	5
BVLOS in sparsely populated environment	3	4	5	6
VLOS in populated environment	4	5	6	8
BVLOS in populated environment	5	6	8	10
VLOS over gathering of people	7	No available		
BVLOS over gathering of people	9			

4) Third, we qualitatively assess the potential for deadly in-flight mishaps (collisions) owing to loss of control during operation by calculating the ARC value. This number is the sum of parts (2) and (3) of the second equation in Figure 2. The SORA methodology categorizes UAS operations into 13 distinct risk collision categories from which the ARC is calculated. The altitude and airspace features (controlled vs. uncontrolled, airport vs. non-airport airspace, lower density vs.

higher density zone) define these groups. The ARC values for the various classes range from a to d. The airspace near an airport, for instance, has an ARC of d due to the high traffic density in the area. In the same way that GRC may be lowered by adhering to certain norms and limiting operational freedom (in terms of time and place), so too can the ARC.

5) Subsequently, we calculate two values for the Specific Assurance and Integrity Levels (SAIL) that describe the degree to which we are certain that the UAS operation will remain under control (the inverse of element (1) in Figure 2). Both the GRC and ARC SAIL values [32] are calculated. Then, the objective with the highest SAIL value is selected to drive the necessary safety goals. Table 2 summarizes the steps taken in the latest iteration of the SORA methodology

Table 2.2: SAIL determination [37]

SAIL Determination				
	ARC			
GRC	a	b	c	d
≤ 2	I	II	IV	V
3	II	II	IV	V
4	III	III	IV	V
5	IV	IV	IV	V
6	V	V	V	V
7	VI	VI	VI	VI

6) Finally, we selected SAIL-level appropriate Operational Safety Objectives (OSOs) with matching robustness levels. The appendix E of SORA [36] provides a complete list of OSOs. This paper provides an overview of the SORA methodology. Briefly, the process includes the following steps: Establish Threat barriers proportional to the severity of the possible Harms caused by a "UAS operation out of control," after the critical level of a UAS operation has been determined. We provide a means of incorporating cybersecurity issues into this methodology.

3. EXPANDING THE SORA METHODOLOGY FOR CYBERSECURITY.

Our suggested remedy, which we refer to as "Harm Expansion" and "Threat Expansion," is divided into these two sections. As a last step in determining the critical level of a specific UAS operation, "Harm Expansion" adds additional harms to the existing risk scenarios being considered. With the help of Threat Expansion, additional cyberthreat scenarios may be considered, and the related Threat barriers for a specific UAS operation can be calculated. Life-threatening harms are the exclusive focus of the typical SORA methodology. Yet, there is also concern about additional harms [11, 32, 35, 38], such as:

3.1 SECRECY VIOLATION:

With the technological advances that have occurred in these last ten years, drones can fly over public buildings and areas that enjoy confidentiality in ministries, sovereign buildings, outposts and military bases. These drones can capture and record video that may reveal a lot of information that is classified as confidential.

3.2 PHYSICAL DAMAGES TO INFRASTRUCTURE

A cyberattack or accident involving an unmanned aircraft might result in the aircraft crashing into a roadway, an electric power line, or a nuclear power plant. For some missions, when planes fly over or close to vital facilities, there is a specific and present danger.

3.3 DIGITAL DAMAGES TO INFRASTRUCTURE

that is believed it a UAS might compromise the safety of essential facilities. An adversary may seize control of a UAS and launch a cyberattack on a target infrastructure using the UAS's network connection, for instance.

3.4 PRIVACY VIOLATION

Because of its compact size, broad operating range, and high performance on-board sensors, a UAS might potentially intrude into private places and gather information [39]. The owner's right to privacy has been invaded. A cyber assault or a system fault might be responsible for the unauthorized disclosure of private information. As an example, law enforcement UAVs may routinely fly over residential areas on route to their assigned missions. It is possible that the privacy of the owners may be breached if the video footage captured on the premises were to be released as a result of a cyber assault

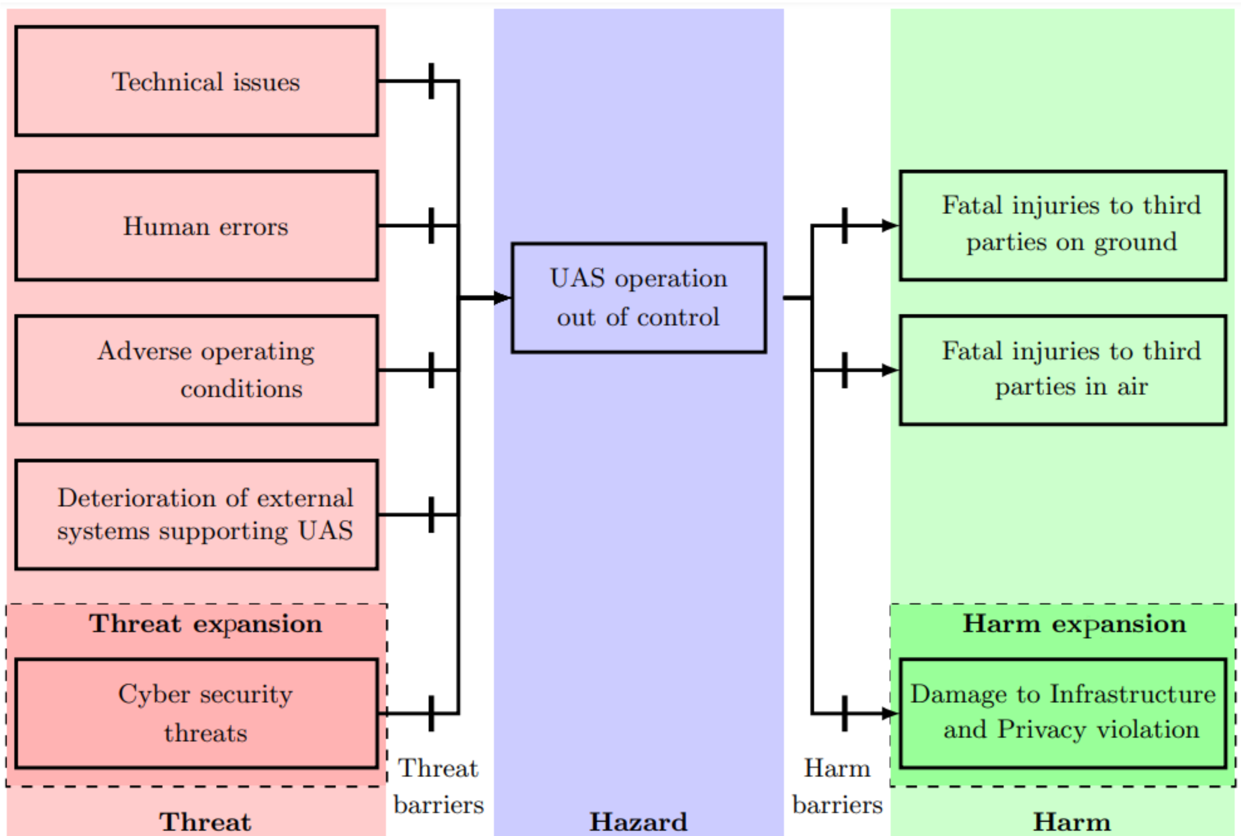

Figure 3.1: Expanded risk model

These new harms, therefore, raise the question of whether or not they should be included in the broader methodology. Our four-pronged approach to mitigating the Harm Expansion's additional harms is as follows:

1) Pick a different harm that requires fixing.

2) Analyze the UAS operation to identify features that increase or decrease the likelihood of the harm of interest.

3) Create quantitative and qualitative likelihood evaluation formulae and tables based on the identified parameters

4) To account for the additional harm's likelihood, the "SAIL determination" phase should be expanded.

Specifically, the Threat Expansion places emphasis on the dangers that are a part of the overall risk picture. We need to identify and categorize new types of cybersecurity threats. To rephrase, we need a classification operation for cyber risks associated with UAS operations. Figure 4 depicts the updated risk model with the additional threat categories added to the threat side to better highlight the potential outcomes of the various scenarios. For each newly identified security risk, we will compile a list of potential countermeasures, or "Threat barriers." After the Threat Expansion has been finalized, the SAIL value will be used to determine which of the proposed Threat barriers should be implemented for a given UAS operation. Unfortunately, the Threat Expansion is still in its early stages of development at this time. But here's how we plan to go about creating this expansion:

1)Take stock of the cybersecurity risks facing UAS that have been highlighted in either real-world example of theoretical studies (e.g., simulations, hypotheses).

2)Based on the results of the study, develop a taxonomy of potential cybersecurity risks

3) Make a complete inventory of the most fundamental Threat barriers for each category of threat in the provided taxonomy. We will classify each barrier into one of three levels of robustness (low, medium, and high) based on the SORA framework. This study also draws inspiration from the most up-to-date cybersecurity countermeasures used in similar but unrelated application domains, such as the automotive and robotics industries

4)Find out how the level of cybersecurity protections for a specific UAS mission will be selected.

4. SECRECY ISSUE AS A HARM EXPANSION

It would be possible to construct Harm Expansion and Threat Expansion independently and then combine them into a single, comprehensive methodology. To conclude this study, we will elaborate on the section of the Harm Expansion that deals with the secrecy concern.

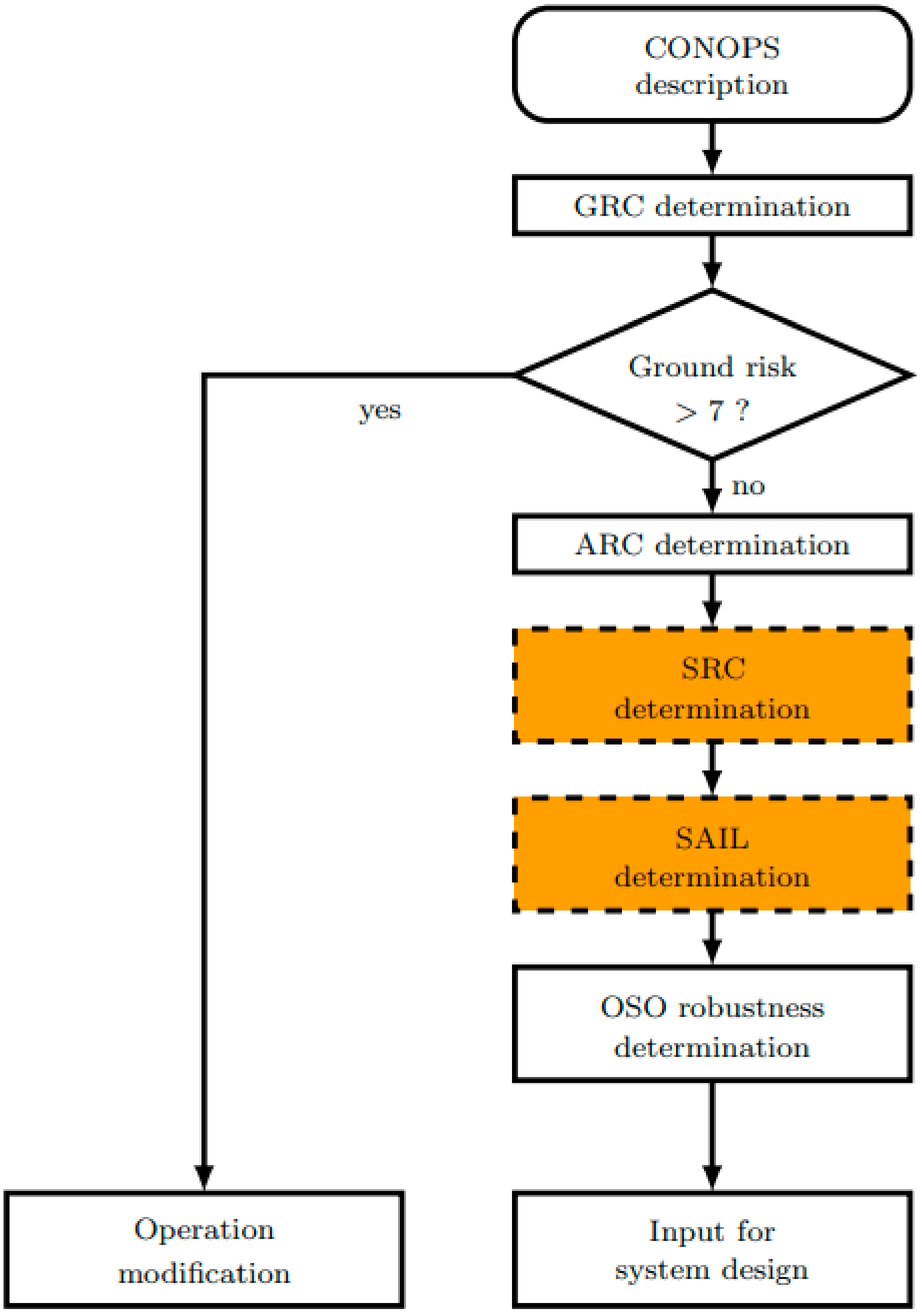

Figure 4.1: The new risk assessment process

One of biggest worries about approving UAS applications is the potential for secrecy to be compromised [32,38,40]. Accordingly, we start our writings with this issue. Since it is challenging to accurately define and address the idea of secrecy [41], we limited our discussion to only these three aspects: There are three types of breaches of secrecy that may occur: (1) the leak of private information, (2) illegal Monitoring and detection without consent surveillance, and (3)intrusion into a secrecy location. Li et al. [42] provide examples of the first aspect. Using drone footage, the authors tested a password-stealing method. References [43– 45] discuss a second related topic. Authors of these works considered how the use of UAS for surveillance can compromise the secrecy of ordinary people. Additionally, Park et al. [44] and Babiceanu et al. [46] established criteria for evaluating privacy breaches of a UAS operation based on the quality of acquired images/videos. Blank et al. [47] handled this final component. In order to prevent unmanned aircraft from accidentally straying into classified regions, the authors suggest a system that can identify such places as flight routes are being developed. Figure 5 depicts our expanded methodology's risk assessment procedure. Secrecy Risk Class (SRC) determination is a new stage in this procedure, and the SAIL determination phase has been adjusted to accommodate it.

Table 4.1: Intrinsic SRC determination

Type of operation	O zone, VLOS	O zone, BLOS	S zone, VLOS	S zone, BLOS	T zone, VLOS	T zone, BLOS
Image detail level						
Monitor	A	B	C	C	C	D
Detect	B	B	C	C	D	D
Observe	B	C	D	D	D	E
Recognize	C	C	D	D	E	E
Identify	C	D	E	E	F	F
Inspect	C	D	E	F	F	F

4.1 OPERATION AREA:

As for the area of operations, it is divided into three areas, areas that are highly classified T and dangerous for the government, the specialized agencies and allies, which are military airports, command centers and operations, sovereign ministries, and the second classification S is secret, and its detection leads to dangers at the tactical and operational levels, and a third section O in which indicate government institutions and bases Military, outposts and gendarmerie points at the operational level

The likelihood of secrecy harms in the event of "UAS operation out of control" is qualitatively evaluated during the SRC determination phase. This likelihood is calculated by first considering three characteristics of the procedure:

4.2 DETAIL LEVEL OF IMAGE:

The likelihood of a violation of secrecy in a building overflown by an unmanned aircraft is proportional to the amount of detail in the photos taken by the onboard camera. So, if the photographs aren't high enough quality, for instance, we won't be able to make out any specifics, which means the likelihood of a violation of secrecy is reduced.

4.3 OPERATION TYPE

: Beyond Visual operation of Sight (BVLOS) operations may increase the likelihood of exposure to aircraft compared to Visual operation of Sight operations (VLOS). Greater flying range in a BVLOS operation may result in more buildings being flown over than in a VLOS operation (with the same space). Also, because the pilot has no visual reference in a BVLOS operation, it is difficult to keep the plane from straying over areas.

With these three characteristics in mind, we were able to calculate the operation's intrinsic SRC (see Table 4.1). Taking into account existing Harm barriers, we arrive at the final SRC in a manner similar to that used to establish the GRC and the ARC. There are three types of secrecy harm barriers that we recommend using: a secrecy protection filter, a restriction on the secrecy area, and an operation-aware notice to the affected parties. Assuming that one SRC level is reduced for every barrier. Unlike the traditional procedure, which only takes into account GRC and ARC in determining an operation's SAIL, the new procedure takes into account these three metrics in establishing SAIL. The SAIL value based on 3 dimensions is referred to as 3D-SAIL, whereas the SAIL value based on 2 dimensions is referred to as 2D-SAIL. The 3D-SAIL method combines the best features of SRC and 2D-SAIL (see Table 4.2).

Table 4.2: 3D-SAIL determination

	2D-SAIL					
SRC	I	II	III	IV	V	VI
A	I	II	III	IV	V	VI
B	II	II	III	IV	V	VI
C	III	III	III	IV	V	VI
D	IV	IV	IV	IV	V	VI
E	V	V	V	V	V	VI
F	VI	VI	VI	VI	VI	VI

5. CASE STUDY

Risk assessments for the unmanned aerial system (UAS) operation described in the EU-funded MULTIDRONE project (https://multidrone.eu) are used to demonstrate our expanded methodology and tool. This is not anything that relates to what we do. However, the aforementioned operation is expanded for investigation since its description is open and comprehensive enough to permit the use of the broader methodology. This operation was initially studied using the SORA methodology by Capit'an et al. [48], which predates our efforts (published in 2017). In 2019, a newer, improved version (version 2) was released. This revision builds on the same idea as the previous one but uses updated evaluative criteria. Version 2 is enhanced in this effort. In what follows, we will use the term "standard methodology" to refer to version 2, and "expanded methodology" to refer to our methodology that accounts for secrecy concerns. For the remainder of the study, we reanalyze the identical MULTIDRONE operation using both the conventional approach and the more comprehensive approach we outlined previously. The procedures of determining the GRC and the ARC are, as noted above, quite similar across the two techniques. The methods to determine SRC, SAIL, and OSO robustness are where you'll see the variations.

Table 5.1: UAS and operation specifications, from the Multidrone project [48, 49]

Main UAS and operation specification	
Frame	DJI S1000+
Autopilot	Pixhawk 2.1
Communication	Thales LTE/Wi-Fi Communication Module
Parachute	Galaxy GRS 10/350
Camera	BMMC + Panasonic Lumix G X Vario Lens
Size	1,45 m
Weight	11 kg
Altitude	10 m
Flight mode	Autonomous
Operation Type	BVLOS

5.1 CONOPS DESCRIPTION

Annex A of the SORA methodology recommends a thorough description of the operation, which may be rather lengthy due to the need to provide details relevant not only to the risk assessment but also to the administrative processes surrounding it. For this reason, we provide just a brief summary of the topic at hand, which should be sufficient for purposes of doing risk assessments. Those interested might look at [48, 49] for further details. In this operation, the drone is tasked with following a human operated vehicle in order to snap photos. Because the operation spans such a vast distance (up to 15 km), the drone travels beyond the line of sight of the pilots and operates in autonomous mode. In order to carry out the operation, we'll be in a sparsely populated location. Drones avoid flying over areas where people may be standing along the flight path. An overview of the planned operation is provided in Table 5.

5.2 GRC DETERMINATION

In this respect, the two approaches are equivalent. We begin by calculating what we call the "intrinsic GRC" of the operation, which is the risk to personnel on the ground apart from any intrinsic protective measures ("Harm barriers"). We consider the operation region to be sparsely populated since the UAV flies in a rural location and does not fly over crowds of people. Based on the operation and size of the vehicle, we used the SORA methodology's GRC table to determine that the intrinsic GRC should be 4. (see Table 1). Then, we look into the operational Harm barriers that may lower the GRC by themselves. There is no emergency response plan in place, and the operation's description doesn't include any discussion of strategic mitigations for ground risk. Because of it, GRC rose. The only Harm barrier used by the operator to mitigate risk is a parachute (Reducing the effect of ground impact). However, it is unclear how the operator verifies that the parachute is set up correctly for the operation at hand. This mitigation is therefore insufficient to significantly cut down on GRC. At the end of the operation, the GRC is 4.

5.3 ARC DETERMINATION

This is the part when the two methodologies are the same. We begin by calculating the initial ARC of the operation, which is the risk of crashing into other collisions without taking Harm barriers into account. The airplane travels at just 10 meters above ground level in uncontrolled airspace that is not very congested, thus the risk of a collision with another aircraft is small. For this reason, the planned operation will have an initial ARC of b and a flying density of 1 in the broadest sense (on a scale of 5 levels [37]). The operator uses mitigation by boundary in the form of a Harm barrier to limit operating volume in order to lower the air risk associated with the operation. The SORA methodology suggests that the Harm barrier is ineffective here since the likelihood of collision is already so low, to begin with (low flight density area). This is why the cumulative ARC never rises over b.

5.4 SRC DETERMINATION

This is a feature of the broader methodology alone. Before addressing any potential barriers posed by Harm, we establish an initial Secrecy Risk Class (SRC) for the potential for a secrecy breach. The majority of the required input data for this procedure has already been supplied in the operation description (see Table 5). However, the required camera minimum field of view is not specified in the operation description (AOV). As stated in Table 6, we might do a rough estimate using the camera's technical specs.

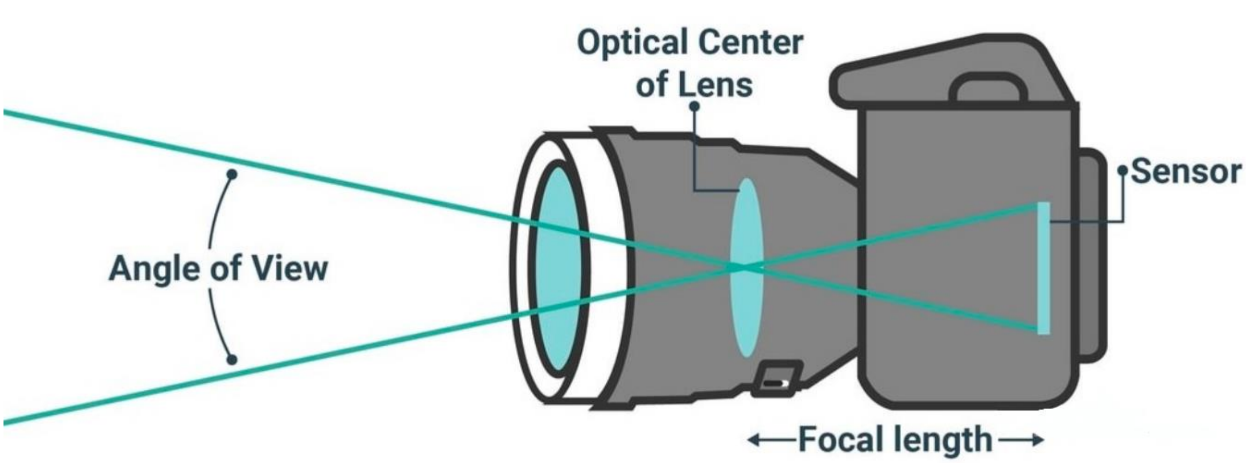

Figure 5.1: Camera specification [50]

Table 5.2: Camera specifications

BMMC camera with Panasonic Lumix G X Vario Lens	
Resolution	2432 x 1366
Sensor size	16.64 mm x 14.04 mm
Focal length	from 14 to 42 mm

The camera's minimal AOV may be determined using the formula:

$$\textbf{minAOV} = \textbf{2 arctan} \frac{\text{sensor width}}{\text{2* max focal length}} = \textbf{11.2°}$$

5.5 SAIL DETERMINATION .

The two methodologies have distinct procedures for this phase. In the conventional methodology, GRC and ARC combine to form the SAIL (2D-SAIL). The procedure has a GRC of 4, and its ARC is b. This means that the SAIL (2DSAIL) is worth III (see Table 2). ARC, GRC, and SRC all come together to form the SAIL in the more comprehensive methodology (3D-SAIL). So it's a cross between 2D-SAIL and SRC. The 3D SAIL rating is IV, with a 2D SAIL of III and an SRC of D. (see Table 4).

5.6 OSO ROBUSTNESS DETERMINATION

Using the SAIL values that were calculated (III from the baseline methodology and IV from the enhanced methodology), we were able to ascertain the degree of robustness of each OSO and the specific goals that needed to be addressed. Some goals in the SORA methodology are more operator-centric than manufacturer-centric since they are meant to assist a UAS authorization application (such as evaluating weather conditions and operator competencies). As a result, this case study addresses important OSOs from the manufacturer's perspective. The information provided by these sources might be used as part of a UAS's development process. And those things are:

5.7 RESULT

In this case study, we used both the normal SORA methodology (version 2) and our expanded methodology to undertake risk assessments for the unmanned aerial system (UAS) operation described in the MULTIDRONE project financed by the European Union. Table 7 provides a summary of the evaluations. This abstract suggests that compared to the conventional methodology, our suggested methodology yields a more stringent SAIL value. Comparing the (SAIL of Generations IV and III). Therefore, taking the secrecy damage into account during the risk assessment requires that we choose a higher robustness level (Medium or High) to achieve the goals (OSO). Because the UAS has a high-performance camera and the operation is taking place in a busy event, this finding makes sense. To rephrase, confidentiality is crucial to the success of this endeavor. The operation and the UAS would need to be drastically altered in order to achieve the goals with even a single more robustness level. These modifications may increase the operation's safety and security, but they may also reduce its efficiency.

Table 5.3: Result Summary

	Methodology	
	Standard SORA	Expanded SORA
GRC	4	4
ARC	b	b
SRC	Not Applied	D
SAIL	III	IV
OSO	Low or Medium robustness level	Medium or High robustness level.

6. CONCLUSION

The scope of the original SORA methodology is broadened in this study to include considerations of cybersecurity. The existing publication for the SORA methodology merely details its use; no explanation of its inner workings is provided. Therefore, we first provided a description of the methodology's idea using our prior understanding of risk assessment and the published literature. After establishing this foundational idea, we present a strategy for further developing the methodology. There are two aspects to the strategy. The first option is called "Harm expansion," and it involves thinking about potential new harms that may arise due to vulnerabilities in cyber security and physical safety. An important worry for the general public's approval of UAS operations is the expansion for "secrecy violation" harm, which we propose to expand in this section. Cybersecurity threats (or assaults) (as opposed to the unintentional threat covered by the standard methodology, version 2) and the appropriate cybersecurity mitigation are the focus of the second section (Threat expansion). This section is still being worked on and will be released at a later date. In addition to the expansion strategy. Finally, we use both the basic and expanded versions of the Systematic Operations Research and Analysis (SORA) framework to a real-world UAS operation to determine its level of risk. According to the findings, the expanded methodology has stricter safety standards that must be satisfied. On the one hand, this implies that the UAS operation must adhere to stricter safety standards in order to make use of the expanded methodology. However, meeting the greater safety threshold may affect the efficiency of a UAS operation since more resources would be needed. Therefore, testing and feedback from professionals in the UAS business are necessary to make the expanded methodology more applicable and widely utilized. There is more to be done in the future to expand the methodology to account for new cybersecurity threats and appropriate cybersecurity goals (Threat expansion). Furthermore, it is important to strike a balance between the goals of safety and cost-effectiveness.

REFERENCES

[1] Tran, T.D., Thiriet, J.M., Marchand, N., El Mrabti, A.: Toward Cybersecurity of Unmanned Aircraft System operations under "Specific" category. In: 2020 International Conference on Unmanned Aircraft Systems (ICUAS), pp. 1433–1441 (2020)

[2] Giones, F., Brem, A.: From toys to tools: The co-evolution of technological and entrepreneurial developments in the drone industry. Business Horizons 60(6), 875–884 (2017)

[3] Vattapparamban, E., Guvenc, I., Yurekli, A.I., Akkaya, K., Uluagac, S.: Drones for smart cities: Issues in cybersecurity, privacy, and public safety. In: 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 216–221. IEEE (2016)

[4] Moskwa, W.: World Drone Market Seen Nearing $127 Billion in 2020, PwC Says. Bloomberg (2016)

[5] Drone market size and forecast 2019-2024. Drone Industry Insights. https://www.droneii.com/project/drone-market-size-and-forecast2019-2024 (2019). Accessed 25 February 2021

[6] European drones outlook study: Unlocking the value for europe. Single European Sky Atm Research Joint Undertaking (SESAR). https://www.sesarju.eu/node/2951 (2016). Accessed 10 September 2019

[7] Drones market research report - forecast 2028. Market Research Future. https://www.marketresearchfuture.com/reports/drones-market1124 (2018). Accessed 25 February 2021

[8] Commercial drones in 2022. Interact Analysis predictions (2018). Accessed 25 February 2021

[9] De Miguel Molina, B., O˜na, M.S.: The drone sector in Europe. In: Ethics and civil drones, pp. 7–33. Springer, Cham (2018)

[10] Bassi, E.: From here to 2023: Civil drones operations and the setting of new legal rules for the european single sky. Journal of Intelligent & Robotic Systems pp. 1–11 (2020)

[11] A-NPA 2015-10: Introduction of a regulatory framework for the operation of drones. European Union Aviation Safety Agency (EASA). https://www.easa.europa.eu/documentlibrary/notices-ofproposed-amendment/npa-2015-10 (2015). Accessed 21 Feburary 2021

[12] Commission implementing regulation (EU) 2019/947 of 24 may 2019 on the rules and procedures for the operation of unmanned aircraft. European Union Aviation Safety Agency (EASA). implementing-regulation-eu-2019947 (2019). Accessed 26 February 2021

[13] Ericson, C.A., et al.: Hazard analysis techniques for system safety. John Wiley & Sons (2015)

[14] Pi`etre-Cambac´ed`es, L., Bouissou, M.: Cross-fertilization between safety and security engineering. Reliability Engineering & System Safety 110, 110–126 (2013

[15] Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., Halgand, Y.: A survey of approaches combining safety and security for industrial control systems. Reliability engineering & system safety 139, 156– 178 (2015)

[16] Raspotnig, C., Opdahl, A.: Comparing risk identification techniques for safety and security requirements. Journal of Systems and Software 86(4), 1124–1151 (2013)

[17] Steve Kremer Ludovic M´e, D.R., Roca, V.: Cybersecurity - current challenges and inria's research directions. Tech. rep., INRIA (2019)

[18] Schneier, B.: Modeling security threats. Dr. Dobb's Journal (1999)

[19] Gorbenko, A., Kharchenko, V., Tarasyuk, O., Furmanov, A.: F(I)MEA-technique of web services analysis and dependability ensuring. In: Rigorous Development of Complex FaultTolerant Systems, pp. 153–167. Springer (2006)

[20] Pi`etre-Cambac´ed`es, L., Bouissou, M.: Beyond attack trees: dynamic security modeling with Boolean logic Driven Markov Processes (BDMP). In: 2010 European Dependable Computing Conference, pp. 199–208. IEEE (2010)

[21] McDermott, J.P.: Attack net penetration testing. In: Proceedings of the 2000 workshop on New security paradigms, pp. 15–21 (2001)

[22] Kornecki, A.J., Liu, M.: Fault tree analysis for safety/security verification in aviation software. Electronics 2(1), 41–56 (2013)

[23] Schmittner, C., Gruber, T., Puschner, P., Schoitsch, E.: Security Application of Failure Mode and Effect Analysis (FMEA). In: A. Bondavalli, F. Di Giandomenico (eds.) Computer Safety, Reliability, and Security, vol. 8666, pp. 310–325. Springer International Publishing (2014)

[24] Abdo, H.: Dealing with uncertainty in risk analysis : combining safety and security. PhD Thesis, Universit´e Grenoble Alpes (2017)

[25] Functional safety Essential to overall safety - An introduction to Functional safety and the IEC 61508 series. International Electrotechnical Commission (IEC), https://www.iec.ch/functionalsafety/explained/ (2015). Accessed 25 February 2021

[26] Guidelines and Methods for Conducting the Safety Assessment Process on Airborne Systems and Equipments. SAE International. / (1996). Accessed 24 February 2021

[27] ISO/IEC 27000 glossary standard. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). http://www.iso27001security.com/html/27000.html. Accessed 26 February 2021

[28] Kobes, P.: Zoom sur la norme international IEC 62443 pour la cybers´ecurit´e des syst`emes num´eriques industriels. In: Cybers ´ecurit´e des installations industrielles. C´epadu`es (2016)

[29] Idrees, S., Roudier, Y., Friedewald, M., Leimbach, T., Andreas, F., Sigrid, G., Olaf, H., Roland, R., Matthias, R., Henrik, B., Ludovic, A., Renaud, P., Gabriel, P., Alastair, R.,

David, W., Benjamin, W.: Security requirements for automotive on-board networks based on dark-side scenarios. Tech. rep., EVITA (2009)

[30] EUROCAE: Airworthiness security process specification ED-202/ DO-326 (2014)

[31] Favaro, J.: Report on the evolution of co-engineering standards. Tech. rep., Electronic Component Systems for European Leadership Joint Undertaking (2018)

[32] Joint Authorities for Rulemaking on Unmanned Systems (JARUS): JARUS guidelines on Specific Operations Risk Assessment (SORA) (2017). Version 1

[33] Nikodem, F., Bierig, A., Dittrich, J.S.: The New Specific Operations Risk Assessment Approach for UAS Regulation Compared to Common Civil Aviation Risk Assessment. In: DLRK 2018 (2018)

[34] European Union Aviation Safety Agency (EASA): Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Commission Implementing Regulation (EU) 2019/947 (2019)

[35] European Union Aviation Safety Agency (EASA): Introduction of a regulatory framework for the operation of unmanned aircraft (2015)

[36] Joint Authorities for Rulemaking on Unmanned Systems (JARUS): Annex E of SORA - Integrity and assurance levels for the Operation Safety Objectives (OSO) (2019)

[37] Joint Authorities for Rulemaking on Unmanned Systems (JARUS): JARUS guidelines on Specific Operations Risk Assessment (SORA) (2019). Version 2

[38] Pauner, C., Kamara, I., Viguri, J.: Drones. Current challenges and standardisation solutions in the field of privacy and data protection. In: 2015 ITU Kaleidoscope: Trust in the Information Society (K2015), pp. 1–7 (2015)

[39] Winkler, S., Zeadally, S., Evans, K.: Privacy and Civilian Drone Use: The Need for Further Regulation. IEEE Security & Privacy 16(5), 72– 80 (2018)

[40] Zhi, Y., Fu, Z., Sun, X., Yu, J.: Security and Privacy Issues of UAV: A Survey. Mobile Networks and Applications pp. 95–101 (2019)

[41] Finn, R.L., Wright, D., Friedewald, M.: Seven types of privacy. In: European data protection: coming of age, pp. 3–32. Springer (2013)

[42] Li, Z., Gao, C., Yue, Q., Fu, X.: Toward drone privacy via regulating altitude and payload. In: 2019 International Conference on Computing, Networking and Communications (ICNC), pp. 562–566 (2019)

[43] Villasenor, J.: Observations from above: Unmanned aircraft systems and privacy. Harvard Journal of Law Public Policy (2013)

[44] Park, S., Lee, K.: Developing Criteria for Invasion of Privacy by Personal Drone. In: 2017 International Conference on Platform Technology and Service (PlatCon), pp. 1–7 (2017)

[45] Bonetto, M., Korshunov, P., Ramponi, G., Ebrahimi, T.: Privacy in mini-drone based video surveillance. In: 2015 11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG), vol. 04, pp. 1–6 (2015)

[46] Babiceanu, R.F., Bojda, P., Seker, R., Alghumgham, M.A.: An onboard UAS visual privacy guard system. In: 2015 Integrated Communication, Navigation and Surveillance Conference (ICNS), pp. 1–8 (2015)

[47] Blank, P., Kirrane, S., Spiekermann, S.: Privacy-Aware Restricted Areas for Unmanned Aerial Systems. IEEE Security Privacy 16(2), 70–79 (2018)

[48] Capit´an, C., Capit´an, J., Castano, A.R., Ollero, A.: Risk Assessment based on SORA Methodology for a UAS Media Production Application. In: 2019 International Conference on Unmanned Aircraft Systems (ICUAS), pp. 451–459. IEEE (2019)

[49] MULTIDRONE project - University of Bristol: Deliverable D2.1: Multidrone media production requirements (2017)

[50] What is focal length and angle of view in photography. Capture the Atlas. https://capturetheatlas.com/what-is-focal-length/ Accessed 23 February 2021